UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/694,416	10/20/2000	Thomas Collins	20206-014(PT-TA-410)	1055

7590 10/07/2004

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SEAL, JAMES	

ART UNIT	PAPER NUMBER
2135	33

DATE MAILED: 10/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/694,416	Applicant(s) COLLINS ET AL.	
	Examiner James Seal	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6, 9-12; and 14-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6, 9-12; and 14-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 October 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The request filed on 28 September 2001 for a Request for Continued examination (RCE) under 37 CFR 1.114 based on parent Application No. 09694416 is acceptable and a RCE has been established. An action on the RCE follows.

2. Objection to the specification for new matter under 35 U.S.C. § 132 is maintained.

3. Claims 4 and 35 have been amended.

4. Claims 7 and 13 have been cancelled.

5. Claims 1-6 and 9-12, 14-61 are pending.

New Matter Objection

1. The amendment filed 16 September 2002 is objected to under 35 U.S.C. 132 because it introduces new matter into the disclosure. 35 U.S.C. 132 states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

2. As per the amendment Col. 4, line 6 the replacement of the phrase "*using* the RSA scheme" "... using a large (many digit) n much faster than heretofore possible", "*extending* the RSA scheme" "... using a large (many digit) n much faster than heretofore possible" . The support relied upon by the applicant is Col. 3, lines 20-26, Col. 4, line 6-12, 32-34 and 52-56. The examiner interprets the first to mean that the present invention is capable of using the RSA scheme to perform encryption and decryption operation using a large (many digit) n much fast than hereforth possible, that is, using an existing system. The replacement discloses using a new system (an extended RSA) for accomplishing this task.

The applicant offers support from Col. 3, lines 20-26 deal with extending the computational speed without any mention of "using a large (many digit) n or an existing RSA system", Col. 4, line 6-12 is the same paragraph that is being amended. Column 4, lines 32-34 discloses a system that employs parallel processing which does not support the change and Column 4, line 52-56 refers to the CPU breaking the encryption/decryption into sub-tasks. None of Attention:Attention: these references are directed at Final Rejection going from an existing RSA system to an extended system and using the extended system "... using a large (many digit) n much faster than heretofore possible" with "extending the RSA scheme". For that reason the examiner does not believe the change is supported and would constitute new material.

3. With regards to the amendment Column 5 line 30, "developed and checked to ensure that each $(p_i - 1)$ is relatively prime to e" the applicant provides support from Column 2, lines 5-10, Col. 3 line 42, col. 4, line 41, Col. 5, line 39, Col. 10, line 65 and col. 11, lines 8-9. Col. 2, lines 5-10 refers to only the standard two prime RSA case. Col. 3, line 42 discloses only $n = p_1 p_2 \ldots p_k$ but no mention of $(p_i - 1)$ relatively prime to e. Col. 4, line 41 discloses $n = p_1 p_2 \ldots p_k$ but no mention of $(p_i - 1)$ relatively prime to e. Col. 5, line 39 $d = e^{-1} \bmod [(p_1 - 1)(p_2 - 1) \ldots (p_k - 1)]$ but no mention of $(p_i - 1)$ relatively prime to e. Col. 10, line 65 discloses where is is relatively prime to $(p_1 - 1)(p_2 - 1)$. The amended claim 1, discloses support of changes of $(p_1 - 1)(p_2 - 1)$ to $[(p_1 - 1)(p_2 - 1) \ldots (p_k - 1)$ using Col. 5, line 30. Col. 11, lines 8-9, discloses that d is the multiplicative inverse to e, and does not address $(p_i - 1)$ relatively prime to e. Further none of the sections recited for support disclose the step of "checking" that each $(p_i - 1)$ is relatively prime to e.

4. With regards to amendment to Col. 5, line 52, no support can be found for digital signature in the original. Claim 9 was quoted as support. Claim 9 does mention a signed message M_A, however claim 10 refers to M_A, as "said *signal message* word signal" in the original patent makes it unclear if claim 9 is support for a digital signature. See means plus function rejection of claim 9. Amendment contains matter no clearly supported by original patent and therefore constitutes new matter and should be taken out.

5. With regards to the amendment to the specification at Column 6, line 24. This amendment to the specification, request that $i \geq 2$ in the original patent with $2 \leq i \leq k$ where k is the number of primes in n. The latter is certainly satisfied by i = k = 2, but k must always be equal to or greater than *three* as specified in the original patent (cf. Col. 5, line 31-32), thus the two statements contradict one another. If the former is what applicant wants, then applicant should supply support for this in the specification or it would constitute new matter.

6. With regards to Col. 6, line 65, in the original patent the sentence reads:

> "In generalized form, the decrypted message M can be obtained by the same summation identified above to obtain the ciphertext from its contiguous constituent sub-tasks C_i."

In the amended version the sentence reads

> "in generalized form, the ciphertext C (i.e., encrypted message M) can be obtained by a recursive scheme as identified above to obtain the ciphertext C form its contiguous constituent sub-tasks C_i."

The examiner notes that the first version reads "the decrypted message M can be obtained" while the second version reads "the ciphertext C can be obtained" which are two distinctly opposite functions. The first version *summation* is required wherein the

second version *iteration* is required. Support for the second version is cited Column 6, lines 1-4; line 26-35; 40-53, and 67 and in particular it would appear that the applicant is making use of "however, it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme." The examiner observes that the use Chinese Remainder Theorem (a summation process) is the focus of the discussion with iteration is given as *the preferred* method for carry out this function, the proposed iteration scheme being given lines 31-39. What follows next lines 40-64 is the standard decomposition for using the CRT for recovering M, then version 1 is given which would be mathematically logical followed by the CRT first equation Column 7 providing the summation process to obtain M. The first sentence at the top of Column 7 again states that the recursive form of the CRT referring to Column 6, lines 31-39 is preferable for greater speed but then returns to finish with the summable CRT. The examine fails to see where any support has been provided for the second version.

The examiner notes from page 39 second paragraph, of applicant's correspondence, support for amendment at Col. 7, line 1 is given as Col. 2, lines 32-34 and 40; Col. 3, lines 22-26, Col. 4, lines 32-34, Col. 6 line 38 and Col. 7, lines 56-58, whereas no support is provided for the amendments regarding Col. 7, line 17 and Col. 7, line 52. As far as the examiner can see, the quoted references do not provide support for Col. 7 line 1 which is a statement of the standard CRT; however, they do not appear to support amendments Col. 7, line 17 (a special case of the CRT) or Col. 7, line 52 (which involves the labels in Figure 1) either. The examiner also notes no support for the

amendment to the specification at Col. 9, line 24. The examiner asked that proper support be supplied for these amendments.

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Objections

7. Claim 4 objected to because of the following informalities:

In line 18 of claim 4, lcm (p1-1, p2-1, ... pk – 1) should read lcm (p_1-1, p_2-1, ... p_k – 1) that is, 1, 2, 3, ..., k should appear as subscripts.

8. Claim 35 is objected to because of the following informalities. In line 5, *p*k should be p_k

Appropriate correction is required.

Claim Rejections - 35 USC § 112

9. Rejection of claims 26-30 under 112 second paragraph is withdrawn with amendments to claims

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claim 1 rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

11. Claims 1-2, 18-19, 32-33, 37, 42-49, 56--61 recites "developing k distinct random prime numbers p_1, p_2, ... p_k where k is an integer greater than 2; providing a number e relatively prime to (p_1 – 1) (p_2 –1) ... (p_k-1)". The patent as originally filed does not disclose

such a condition for $k \geq 3$. The only reference found in the original reference is given on column 5, line 33, which recites "Then, three or more random large, distinct primes numbers, $p_1, p_2, \ldots p_k$ are developed and checked to ensure that *each is relatively prime* to e", which alleges the primes should be relatively primed to e, and thus does not supported by the original patent. Claims 1-2, 18-19, 32-33, 37, 42-49, and 56—61 are rejected under new matter.

12. Claims 3, 4-6, 9-12, 14-19, 28-37, 40-41 recites "developing k distinct *random* prime numbers $p_1, p_2, \ldots p_k$ where k is an integer greater than 2; providing a number e relatively prime to lcm $(p_1 - 1, p_2 - 1, \ldots, p_k - 1)$" or the lowest common multiplier. The patent as originally filed does not disclose such a condition for $k \geq 3$ as disclosed above. The only reference found in the original reference is given on Column 5, which recites "Then, three or more random large, distinct primes numbers, $p_1, p_2, \ldots p_k$ are developed and checked to ensure that each is relatively prime to e". The applicant has not provided support for this new limitation either from the original patent are from the RSA patent. Claims 3, 4-6, 9-12, 14-19, 28-37, 40-41 are rejected under new matter.

13. Claims 1-61 rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

14. Claims 1-61 now recite "developing k distinct *random* prime numbers $p_1, p_2, \ldots p_k$ where k is greater than 2... ". The term *random* with regards to the primes $p_1, p_2, \ldots p_k$ is cited once in the original patent Column 5, line 31 and does not appear in the RSA patent with regards to the primes. Claims 1-61 are rejected under new mater.

15. As the applicant points out in the last paragraph of page 46 and the top of page 47 of his correspondence, it is clear that the applicant now believes that "The *randomness* and distinctness attributes of the k prime numbers will materially improve the security in any cryptographic system with RSA public key encryption." If this were the intent of the original patent, the original patent does not support this view.

16. The rejection of claims 7 and 13 under 35 U.S.C. 112, first and second paragraph, for lack of written decryption is withdrawn as they have been cancelled.

17. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

18. Regarding amended claim 9, the word "means" is preceded by the word(s) " $M_{1s} \equiv M_1{}^{d_1} \bmod n_1$ " in an attempt to use a "means" clause to recite a claim element as a means for performing a specified function. However, since no function is specified by the word(s) preceding "means," it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph. See *Ex parte Klumb*, 159 USPQ 694 (Bd. App. 1967).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1-7, 9-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest et. al. (US 4,405,829 A) henceforth RSA, and further in view of Rivest et. al. A Method for Obtaining Digital Signatures and Public-key Cryptosystem, Communications of the ACM, 21(2) February 1978, henceforth Rivest and further in view of Knuth, The Art of Computer Programming vol. 2 page 179.

20. As per amended claim 1, the limitation of a method for processing messages in a communication system with RSA public key encryption an alternative embodiment of the present invention (see Figure 6, Abstract line 1 of Column 4, lines 15 through Column 5, lines 11, RSA), such that three or more primes $p_1, p_2, p_3, \ldots, p_k$ are generated, such that $k > 2$ (Column 13, lines 30-31) then using the present invention (Column 13, line 29) provided and e relatively prime to $\phi(n)$ (Column 13, lines 42-44), $\phi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1)\ldots(p_k - 1)$, that is, relatively prime to $(p_1 - 1)(p_2 - 1)(p_3 - 1)\ldots(p_k - 1)$ and generating from the product of these primes and integer n which will be the resulting modulus n (Column 13, line 30-31, line 34) using the provided e and n together with a message M where $0 \leq M \leq n-1$ (Column 4, line 26), and the RSA encryption algorithm $C \equiv M^e \bmod n$ (Column 4, line 59, RSA) to generate a cipher text C, decrypting C at the intended recipient (Column 6, 29-31) having available to it

21. With regards to what the applicant regards as his invention and how it differs from the RSA patent, we consider first applicant's comments page 46 of amendment. The recitation in claim 1 includes developing k distinct random prime numbers $p_1, p_2, p_3, \ldots, p_k$, where k is an integer greater than 2, and further includes the fact that the modulus n is a composite number equaling the product $p_1p_2p_3 \ldots p_k$. Namely, claim 1 recites that k is an

integer greater than 2 that is k > 2 and the k primes numbers are random and distinct. Moreover, claim 1 recites that the modulus n is provided from a product of the k prime numbers. Contrast this (claim 1) recitation with selecting a modulus n and then factoring n to the k prime numbers. It is clear from this that the applicant believes that RSA teach selecting a modulus n and then factoring n as oppose to selecting k distinct random primes.

22. RSA patent does not disclose the method by which they choose primes; however, on page 123, column 2 at the beginning of section B, Rivest states "each user must (privately) choose two large random prime number p and q to create his own encryption and decryption keys" Thus it is clear that Rivest does intent to use large random primes for RSA cryptosystem in general. Rivest states to protect against sophisticated factoring algorithms, each prime should *differ in length by a few digits* (Rivest, page 124 third paragraph). Thus Rivest teaches randomness and distinctness for security of the primes for RSA cryptosystems.

23. RSA patent recites a different embodiment (Column 13, lines 30-31) in which the modulus n is a product of three or more primes (not necessarily distinct primes). RSA further goes on to state that decoding may be performed modulo each of the prime factors of n (thus breaking the calculations into a series of subtacks involving the factors of n and not n) and then combining the results using "Chinese remaindering" (that is the Chinese remainder theorem henceforth CRT). However, only in the case of distinct primes can the decoding problem be performed using the CRT. In the case of non-distinct primes one would need in addition Hensel's Lemma (or a generalization by Hensel of p-adics, see Knuth vol 2, page 179). Thus it is clear that the RSA patent is referring to the case of distinct primes. Claim 1 is rejected.

24. As per claim 2, the RSA patent teaches that in any RSA public key cryptosystem, may be implemented in an alternative embodiment of the present invention by making n the product of k random and distinct primes, such that, the decryption of ciphertext C should be accomplished by $M \equiv C^d \bmod n$ is disclosed Column 13, lines 44-46 and d is chosen as the multiplicative inverse of e such that $ed \equiv 1 \bmod L$, L = least common multiple, which in the case of k primes is $L = \text{lcm}\{ p_1 - 1, p_2 - 1, \ldots p_k - 1 \}$) (Column 5, lines 1-15, Column 13, line 30-31). Claim 2 is rejected.

25. As per claim 3, RSA patent teaches that in any RSA public key cryptosystem may be implemented in an alternative embodiment of the present invention with the limitation of j communicating terminals on a communication system, with encrypting key $E_i = (e_i, n_i)$ and decryption keys $D_i = (d_i, n_i)$ i = 1, 2, ... j, (Column 8, lines 22-27) wherein for each terminal i, e_i, d_i, and n_i are defined as in claims 1 and 2 (see above) wherein the message M_i corresponding to a number representative of a message-to-be-transmitted from the ith terminal and in particular terminal 1 transmits a message M_1 to terminal 2 by breaking the message M into blocks M" where $0 \leq M_1" \leq n_2 - 1$ (Column 4, lines 31-35; Column 8, line 39) message to ciphertext using $C \equiv M_1"^{e2} \bmod n_2$ (Column 8, line 56). Claim 3 is rejected.

26. As per claim 4, the RSA patent teaches that in any RSA public key cryptosystem, may be implemented in an alternative embodiment of the present invention by making n the product of k random and distinct primes, such that, the limitation that the decryption of the ciphertext C between two terminals (as defined in claim 3) is decrypted according to $M' \equiv C^d \bmod n$ (where d and n are defined as above) and where M' corresponds to the decoded ciphertext block is disclosed (Column 8, line 43). Claim 4 is rejected.

27. As per claim 5, the limitation of a communication system incorporating the encryption of messages as claim 3 and the receipt and decryption of messages as claim 4 form a *first* (or transmitting) terminal to a second terminal and are therefore rejected on grounds analogous to those used to reject claims 3 and 4.

28. As per claim 6, the limitation of a communication system incorporating the encryption of messages and the decryption of messages from a second (transmitter) terminal to a first terminal (receiver) and a blocking means (Column 4, line 33) and are therefore rejected on grounds that the limitations of claim 6 combine the limitations of claims 3 (an encoder for encrypting messages to be transmitted) and 4 form (decoding messages encrypted in the manner of three) and are rejected in view of the same art of record.

29. Claims 7, 8 and 13 are cancelled.

30. As per claims 9 and 10, the limitation of sending signed messages between terminals is disclosed by Rivest Column 5, lines 18-50 and Column 8 lines 56-67. Claims 9 and 10 are rejected.

31. As per claim 11, the limitation that the communication system is comprised of stations capable of generating ciphertext is disclosed by Rivest Column 8, lines 33-39 and Column 10, line 28-34. Claim 11 is rejected.

32. As per claim 12, the limitation that such stations transmit ciphertext is disclosed by Rivest Column 8, lines 33-39, Column 10, lines 11-24, lines 28-34, and Figure 4. Claim 11 is rejected.

33. As per claims 14 and 15, a method of processing messages by *selecting* a public e which is used with the relationship $C \equiv M^e \bmod n$ (claim 14) and (claim 15) *establishing* a

private key portion $d \equiv e^{-1} \bmod L$ respectively is disclosed by Rivest Column 6, lines 21-37. Claims 14 and 15 are rejected.

34. As per claim 16, a method of processing messages selecting a public key e and establishing a private key $de \equiv 1 \bmod L$ where n is a product of 3 or more *distinct* primes and decoding ciphertext using the relationship $M \equiv C^d \bmod n$ is disclosed by Rivest Column 6, lines 21-37 and Column 13 lines 29-31, lines 41-43. Claim 16 is rejected.

35. As per claim 17, the limitation $M \equiv C^d \bmod n$ is disclosed by Rivest Column 13 line 46. Claim 17 is rejected.

36. As per claim 18, selecting a public key e and corresponding private key $d \equiv e^{-1} \bmod \phi(n)$ and encrypting M with the private key produces a signed message M_s is disclosed by Rivest Column 8 lines 56-67. claim 18 rejected.

37. As per claim 19, the limitation that the signed message can be verified by the public key is disclosed by Rivest Column 9, line 3. Claim 19 rejected.

38. As per claims 20-23, the limitations of a multiprime RSA cryptosystem n = pqrs... whereby the speed of the cryptographic process is increased is disclosed by Rivest Column 13, line 33. Rivest discloses the use of the CRT, which because of its mathematical form allows the breaking up of the decryption process into a series of subtasks ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$ ...). This puts the calculation in terms of subtask which are then automatically in a form to utilize parallel processing in the calculation and because the primes used in each subtask are small, increased speed is a consequence. Claims 20-23 are rejected.

39. As per claims 24, 25, 28, 30, and 32, in as far as the examiner understands the limitation, "fewer computational cycles" for a multiprime RSA cryptosystem, is disclosed by Rivest as a results of the CRT as discussed above. With smaller primes, the necessary computational cycles would also be less, for example using the Euclidean algorithm or the CRT. Claims 24, 25, 28, 30, and 32 are rejected.

40. As per claims 26, 27, 29, 31, and 33, in as far as the examiner understands the limitation, "faster than heretofore possible" for a multiprime RSA Cryptosystem is disclosed by Rivest as a results of the CRT as discussed above. If the number of computational cycles is fewer that would imply that the calculation are completely faster. Claims 26, 27, 29, 31, and 33 are rejected.

41. As per claims 34-39, in as far as the examiner understands the limitation, a "method compatible with RSA" with the multiprime RSA is disclosed by Rivest. Rivest would allow a standard two prime RSA cryptosystem to communicate with a multiprime RSA cryptosystem as only the public keys (e, n) are used for encryption by the other party machine and no use of the factorization is used in the process. Claims 34-39 rejected.

42. As per claims 40-41, the limitation of a cryptographic method for local storage of data by a private key is disclosed by Rivest Column 6 lines 50-57 and grounds in claims 14 and 15. Claims 40-41 rejected.

43. As per claim 42, the limitation of a communication system with a plurality of stations over a communication link (channel) is disclosed by Rivest Abstract.

44. As per claim 43, the limitation of a system for processing message by encrypting a first message $C \equiv M^e \bmod n$ and also being able to decrypt a second encrypted message C' into M' is disclosed by Rivest (see Figure 4). Claim 43 is rejected.

45. As per claims 44 and 45, the limitation of breaking the encryption/decryption into subtasks is a consequence of the application of the CRT which Rivest discloses in Column 13 line 33. Claims 44 and 45 rejected.

46. As per claim 46-49, the limitations of data bus (Figure 3), processor(Figure 3), memory (Figure 1&3), exponentiator (Figure 3, element 22) parallel processing (Column 13, line 33) is disclosed by Rivest Column 9, lines 6-58; Figure 3. DES implementation for session keys is disclosed by Rivest (Column 3, lines 23-30 and Column 1, lines 42-45, Column 14, lines 26-28). Claims 46-49 rejected.

47. As per claims 50-55, limitations involving subtasks is a consequence of the CRT which breaks up the decryption process ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$ ...) into subtask (Column 13, lines 31-34) disclosed by Rivest. Claims 50-55 are rejected.

48. As per claims 56-61, it would be inherent that Rivest would provide a means of key development or key generation in order to prevent degrading of security of the encryption system from overuse of keys. Claims 56-61 are rejected.

49. Schwenk discloses encryption and decryption using a form above using the factors and coefficients and the CRT to assemble the results (Column 2, lines 25-67and Column 3, lines 1-35.

50. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 rejected under 35 U.S.C. 102(b) as being anticipated by Vanstone and Zuccherato (*Using four-prime RSA in which some bits are Specified*, Electronic Letters, 30(25), 16 August 1994).

51. Vanstone et. al. discloses an device for reducing key size for transmission to a group of users in a communication system using 4 primes RSA for increased speed and security

(Vanstone et. al., column 1, page 2118,). Vanstone system is in response to the recently advances in factoring which make integers n, in the range 2^9 = 512 bits insecure and suggests going to 2^{10} = 1024 bits with 4 randomly selected primes, each prime contains about 250 bits in both cases (Column 1, first four sentences). There is nothing in the Vanstone method which precludes extending to more bits or more primes in order to address future security needs. Vanstone selects random primes even though he makes bit assignments in an expanded product. Vanstone further discloses use of the CRT for decryption ($M = C^d \bmod n$, $0 \leq M \leq n - 1$), which because of its mathematical form of breaking the decryption process into a series of subtasks ($M_p \equiv C^d \bmod p$; $M_q \equiv C^d \bmod q$; $M_r \equiv C^d \bmod r$; and $M_s \equiv C^d \bmod s$) allows implementation of parallel processing in the calculation. Furthermore the form of the CRT indicates that the primes are distinct. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 rejected.

52. The examiner wishes to thank the applicant for pointing out the typo, that the rejections under Nemo and Slavin should have been under 102 (a) not 102(e). The rejection stands now as a 103(a) with the amendments to the claims. If the applicant wishes to swear behind these references, he should do so.

53. Claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nemo (RSA Moduli Should Have 3 Prime Factors), and further in view of Rivest et. al. (A Method for Obtaining Digital Signatures and Public-Key Cryptosystem). The Nemo article was submitted in the original Collin's application, and although no publication date mentioned in the parent case, the footnote at the bottom of the first page of the article, list a date of August 1996.

54. Nemo discloses an apparatus/method for use in networks and smartcard of using 3 primes (three primes) RSA for increased speed (section 4.1) and security (section 5) applicable to networks (section 4.2) using digital signature for validation (section 4.2, last paragraph and section 6) in a standard digital architecture (section 4.1). The speed increase due to the CRT and smaller moduli see Section 3.1 and 4, in particular parallel processing using subtasks (see especially 3.1).

55. Nemo does not discuss how to choose the primes in his article; however, Rivest article teaches that RSA public key cryptosystem should use distinct and random primes. Modivation for distinct random primes is to be found in the speed and security of such a method. Claims 1-6, 9-12, 14-31, 34-36, 38-44, 50-61 are rejected.

56. Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are ejected under 35 U.S.C. 103(a) as being unpatentable over Itakura and Nakamura, A Public-Key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No 71, October, and further in view of Rivest, A Method for Obtaining Digital Signatures and Public-key Cryptosystem.

57. Itakura et. al. discloses an apparatus/method for cryptographic communications extending the two prime public key encryption to using three primes (page 4, Column 1)using 3 randomly selected distinct primes RSA for which the encryption is carried out $C \equiv M^e \bmod n$ and $n = pqr$ and $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$ where e is relatively prime to and smaller than (p-1)(q-1)(r-1) (page 4 and where decryption is carried out by $M \equiv C^d \bmod n$ where $0 \leq M \leq n-1$ and capable of performing one or more digital signatures per document $S \equiv M^d \bmod n$ (See page 4 section 3) for increased speed and security of digital multisignature applicable to public-key cryptosystem in conjunction with a communication system for a

plurality of users (network, see Figure 1, see Abstract Electronic mail). Itakura et. al. use a random number key generator to develop keys (Figure 1, section 3.1) Claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-61 rejected

Claim Rejections - 35 USC § 102

58. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. 102(a) as being anticipated by Salvin.

59. Salvin discloses a method of encrypted communication (Abstract) using four prime RSA $n = p_1xq_2,xp_1xq_2,$ in which the four primes are selected at *random* and all of which *all are different values* (Column 7, lines 35-67in particular lines 37-38)and corresponding public and private keys e and d (see figure 3, Column 4, lines 31-38 applied to a network with a plurality of users (Figure 1). Salvin further discloses the use of the CRT to speed up the 4 prime decryption (Column 9, lines 44-47) whose speed is inherent from the breaking up the modular exponentiation into smaller primes and parallel subtask.

Response to Arguments

Applicant's arguments filed 1 December 2003 have been fully considered but they are not persuasive.

60. With regards to Nemo, RSA Moduli Should Have 3 Prime Factors, © August 1996 (as per footnote page 1), Applicant asserts that the Captain Nemo paper cannot be accreted as being published on August 1996 since the paper was submitted under a pseudonym and under what appears to be a fictitious publication name "Scientific Bulgarian". However Applicant's argument relies on the false assumption is a fictitious publication renders no meaning to the stated publication date August 1996. On the contrary "scientific Bulgarian" is well known in the art as a indication of a paper being published under, "Copyleft for scientific papers" (see citations's), As can be seen, the first footnote of the Captain Nemo paper fully complies with the directives of copyleft, and thus fully must be accepted as valid evidence that the Captain Nemo paper was indeed published August 1996. Further note that academia is replete with many pseudonyms without detracting from their validity e.g. "Publius" as author of *The Federalist*, "Anon et. al." as the original author of the Transaction Processing Benchmark Papers (It evolved from the DebitCredit test originally published in 1984. This effort was spearheaded by Jim Gray but had so many contributors from industry and academia that the author on the paper was given as Anon et al. This paper struck a chord in the database community.), "Nicholas Bourbaki" the famous French formalist mathematical school and was a Professor at the University of "Nanciago" (as many of its members that wrote of the pseudonym of Bourbaki were from the University of

Nance and the University of Chicago) and final "Student" (for William Sealey Gosset the famous statistician of Guinness Brewery).

61. With regards to new subject matter, see Examiner's Action page 7 second paragraph, applicant has not provided support for inclusion of that material (see action for reference to material in question) and the one reference supplied in the original correspondence of applicant supplies one reference in the specification which does not seem to fit any of the material which the applicant wishes to add to the specification.

62. With regards to the inclusion of the term *digital signature* in the claims, the examiner notes that the support provided from claim 9 in the original patent is thrown into doubt when read in light of claim 10 of the original patent. The examiner further notes that digital signature of certain public key systems such as Elgamal is not performed by encrytpting M with the private key. Some public key systems such as the lattice based NTRU has not even been able to define a secure signature scheme based on the private key or any other process. Further the examiner notes that the use of the private key may be used for encryption rather than decryption as a form of copy protection. So without a clear statement that he did mean this to be applied as a digital signature the examiner is not satified that this isn't new material. This also does not cure the problem of the 112 means see page 11 #34.

63. With regards to the terminology "extending" versus "using" RSA, the latter being the terminology in the original patent, the examiner notes (see Column 13) that the

original RSA patent does teaches more than 2 primes (see column 13) and so the applicatant suggesting that his proposal to use more than two is extension of the original RSA does not follow. RSA does suggest using more than two primes and thus it is not an extension but using a teaching of RSA.

64. With regards to the change of the notation concerning the inequalities, please see Action #15 and note k is the number of primes in n which in applicant specification is always greater than 2 and yet the proposed change $2 \leq i \leq k$ would allows the case $i = k = 2$, which is a contradiction with the first which I do not believe is the intent of the applicant at least from the standpoint of the specification. The examiner suggest if the applicant wish to stick with this form then it should be written as

$$2 < i \leq k$$

where it is now clear that i and k can never take on the value of 2.

65. With regards to the different forms of the CRT, the examier is well aware of the different forms of the CRT and in fact a careful reading of # 16 should reveal this. The should also point out that Gauss was not the first to purpose the Chinese Remainder theorem, that it was prosed by both Indian and Chinese mathematicians century earily. In particular Sun Tzu was apparently the first chinese mathematician according to Dickerson to have purposed it. And as Knuth points out the application of these principles in hardware for the purpose of speeding up calculations goes to Svoboda and Valach in 1955 (see Knuth pgs 254-257 or Handbook of Applied Cryptography Menezes et. al. 1996 section 14.7). Further Gerner has been known as an alterjate form of the CRT since 1959 according to Knuth. Certainly both of these forms were known well

before the applicant and are discussed in Knuth. What the examiner is pointing out in #16 is that the original patent refers to both forms of the CRT, the difficulty is that the part in content seems to follow from the part discussing the use of sumation not iterative or recursive form and can not be claimed original with the inventer.

66. With regards to the discussion of randomness page 7 of applicant's correspondence, In re Chu does not apply. We are not talking about selecting three or more random primes as an advantage, but as a stated limitation. With regards to RSA/Rivest and Knuth, applicant states that Rivest suggest choosing distinct random primes to protect against sophisticated factoring algorithms. So Rivest clearly teaches random selection of primes is necessary to prevent sophisticated factoring attacks. Selection of random primes would also hold for the same reason in the three or more case even if some of the primes or multiple. If on the other hand in re Chu did apply, for the sake of argument, then one could claim the RSA patent teaches the applicant invention without further discussion.

67. With regards to Knuth, Knuth points out that only in the case of distinct primes can the decoding problem be performed using the CRT *alone*. In the non-distinct case one must rely on the CRT *and* the Lemma of Hensel or some equivalent means such as the CRT and p-adics. Clearly, Rivest, Shamir, and Adelman are well known mathematicians in the own right as well as cryptographers, and when in Column 13 line 33 they refer to two well known distinct cases (not *necessarily* distinct primes) and followed by "Decoding may be performed modulo each of the prime factors of n and the results combined using Chinese remaindering ...", they are teaching both

embodiments. Thus RSA clearly is teaching distinct primes here. The motivation for distinct randomly choosen distinct multiprime comes from the same authors and thus is not pieced together. Knuth is only used to elaborate on the mathematics of the art and provides insight into how various algorithms achieve speed over more traditional approach.

68. With regards to Vanstone and Zuccherator, With regards to Vanstone and Zuccherato, their paper teaches Using four-primes RSA (Column 1, page 2118, pagraphy, note the use of the word "using" RSA as opposed to "extended" RSA) and in particular, the primes (Column 2, page 2118 first complete paragraph teaches that primes of the form p = c + a are selected at random by choosing (selecting Column 2, third paragraph) a random for a given c and then searching for a given prime in the neighborhood. The primes selected in this manner are thus random as there is no determististic distribution of primes known. Again Vanstone et. al. teach the CRT (Column 1, second pargraph page 2118) teaching the use of distinct primes. Hence the four primes of Vanstone et. al. are distinct randomly selected primes. With regards to Nemo, the applicant has alleged that this prior art is sucspect because the original patent listed listed it with no date. The examiner had no difficulty finding a date and reference for this document and does not believe that it should not be considered as art simply because no date was listed in the oin the original patent. As the Applicants claim to have provided this paper, it would help to clear the record if the applicant would provide for the record the origin and probaly date of this article. As the examiner does not see at this time any evidence other than the original patent list it as undated that

would disqualify this document the rejection will be maintained pending any information that the applicants might supply on the original and or date of publication. As suggested previously the applicants are encouraged to issue a terminal disclaimer. As far as the journal "Scientific Bulgarian" the examiner will check into this further but the applicant should supply any evidence other than the names that this document should not be taken as face value. With regards to Itakura and Nakamura in view of Rivest, Itukura et. al. is used for the teaching of multiple primes and the teachings of Rivest for random distinct primes as a method to provide a secure public key cryptography.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

James Seal

James Seal

September 30 2004